HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/81C

7 September 2017

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Operational Incidents Watch

The Hong Kong Monetary Authority (HKMA) published today the enclosed eighth issue of Operational Incidents Watch (see enclosure).

The Operational Incidents Watch is a periodic newsletter to share with the industry the major lessons learnt from selected significant operational incidents that have happened in the banking sector. It aims at facilitating authorized institutions (AIs) and members of the public to stay alert and to take appropriate measures to prevent similar incidents from happening to them. The HKMA expects the senior management of AIs to take steps to ensure that their business lines or operational risk management functions will take into account the incidents described in the Operational Incidents Watch in reviewing and enhancing where necessary their institutions' risk management controls.

If there are any questions on the Operational Incidents Watch, please contact Mr Chi-kau Lee at 2878-8271 or Ms Debora Chan at 2878-1593.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)

Encl

55th Floor, Two International Finance Centre,
8 Finance Street, Central, Hong Kong
Website: www.hkma.gov.hk

香港中環金融街8號國際金融中心2期55樓
網址：www.hkma.gov.hk

Issue No. 8
7 September 2017

Operational Incidents Watch is a periodic newsletter published by the Banking Supervision Department of the Hong Kong Monetary Authority (HKMA). It summarises the major lessons learnt from selected operational incidents[1] that have happened in the banking industry and led to impact on relevant customers or material financial losses of the authorized institutions (AIs) concerned. It aims at facilitating AIs and members of the public in Hong Kong to stay alert and to take appropriate measures to prevent similar incidents from happening to them.

In this newsletter, the modus operandi or the factors and key control loopholes leading to two operational incidents are outlined. These incidents involved: (a) deficient practices in ascertaining insurance protection for bill discounting business and (b) misappropriation of a customer's funds by a staff member using a returned ATM card.

Deficient practices in ascertaining insurance protection for bill discounting business

Deficiencies of an AI in (i) ensuring the ongoing insurance coverage for a trade bill purchased from an exporter and (ii) processing an insurance claim on an overdue bill caused the AI to suffer heavy losses when the importers defaulted.

Modus operandi / factors leading to the incident

The AI purchased an export bill from a customer. The underlying exposure to the drawee of the bill (i.e. the importer) was covered by an export credit insurance policy underwritten by an insurance company. The importer was unable to settle the bill when it was due. Subsequently, the AI approached the insurance company

[1] Because of sensitivity, the incidents mentioned in this newsletter may be prepared on the basis of synthesis of multiple incidents and certain details of the incidents may deliberately be omitted.

to claim on its exposure to the importer. However, the insurance company informed the AI that the insurance covering the concerned importer had been cancelled at some time after the bill was purchased by the AI and the cancellation notification had already been issued to the customer. As such, the AI fell out of the insurance protection and was unable to recover the loss.

In a separate case where an importer failed to settle a bill purchased by the AI, the AI lodged an insurance claim with the insurance company. It was later discovered that the claim was made beyond the time prescribed in the insurance policy (i.e. within 210 days past due). Therefore, the insurance company refused to compensate the AI for the financial loss.

Control loopholes and lessons learnt

The AI did not have proper procedures to ensure the continued validity of insurance policies in mitigating the risk arising from its bill discounting business. This could render the AI's interest unprotected, should the relevant importers default on their payments. Specifically, the AI concerned in the first case would be able to reduce its financial loss by taking suitable steps to prevent the insurance policy from being cancelled without its knowledge. In the second case, if the AI had filed the insurance claim before the deadline specified in the insurance contract, the financial loss could have been avoided.

Misappropriation of a customer's funds by a staff member using a returned ATM card

The incident involved possession of a customer's e-banking login information by a staff member of an AI, and control deficiencies of the AI in processing the issuance and return of ATM cards.

Modus operandi / factors leading to the incident

The customer was not familiar with the AI's e-banking platform. He passed his e-banking login name and password to a branch staff member of the AI, and asked the staff member to login his e-banking account at the branch and conduct investment transactions in accordance with his instructions. The staff member retained the e-banking login information since then.

A couple of years later when the customer opened another account with the AI, an ATM card and a Personal Identification Number (PIN) were issued to him for the new account. As the customer did not need the ATM service, he returned the card and PIN to the staff member for cancellation. Using the customer's e-banking login information, the staff member conducted online fund transfers from other accounts of the customer to the newly opened account, from which the staff member withdrew cash using the ATM card and PIN returned by the customer.

The fraud remained undetected for a few months until the customer requested for his account statements and identified the unauthorised transactions. The AI had to compensate the affected customer for his loss.

Control loopholes and lessons learnt

i. The internal fraud could have been avoided if the AI had had in place proper controls in handling the issuance and return of ATM cards and PIN at branch counters. In particular, the relevant processes should preferably be handled by staff responsible for ATM card custodian (the "custodian staff"). The custodian staff should confirm with customers the need for ATM services before issuance, and dispose of returned cards (and PIN) in front of the customers. If custodian staff cannot be arranged for these processes, frontline staff should be required to carry out the work only in the presence of their supervisors.

ii. In addition, the AI should have a policy requiring frontline staff to refrain from retaining customers' login information even if it is provided by customers voluntarily. Customers should be advised to keep their e-banking login password and PIN secret and not to share those with anyone including the staff of the AI. Apart from passing on this advice to customers when the password and PIN are issued, the AI may consider providing reminders from time to time through different channels (e.g. display on the ATMs, the AI's website, or as part of promotional emails sent to customers).